D omain-based
M essage
A uthentication
R eporting
C onformance

APPLYING LIFE'S GOLDEN RULE TO CURB SPAM AND PHISHING

Email Spoofing and Related Issues

- Message headers have no checks by defaut.
- Email messages with forged sender addresses.

Email Spoofing and Related Issues

- Complex email infrastructures discourage use of authentication.
- Domains with mixed deployments for message authentication still force mail receivers to decide between desired and undesired messages.

Email Spoofing and Related Issues

- Receivers are adverse to rejecting messages, generally.
- Senders get no feedback on their efforts to clean up their infrastructure.

Sender Policy Framework (SPF)

- System to verify authorized mail senders.
- Domain owners publish DNS TXT record of authorized senders.
- Mail receivers query DNS TXT record of domain in RFC5321.MailFrom (bounce address, envelope-address, return-path) field to verify IP of sender.
- Gives mail receivers some basis for rejecting mail.

Domain Keys Identified Mail (DKIM)

- Message authentication with digital signatures.
- Mail senders attach tag-value pairs to the message necessary for verification.
  - s= selector for DNS record of public key
  - d= domain that signed the message
  - Others for hash, version, algorithm, header fields, canonization algorithm, etc.

Domain Keys Identified Mail (DKIM)

- Mail receivers query DNS TXT record for the public key at <selector>._domainkey.<domain>.
- Reliable verification of signing domain identity and of message integrity.

DKIM-Signature: header

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=tvc.texas.gov;
s=selector1; h=From:Date:Subject:Message-ID:Content-Type:MIME-Version;
bh=pbiiVj4pVzXEiG0IFpnDmJ8Djrf0VPqouDUPWi9MglY=;
b=fAkkbsj6c9lWWiBN7JmbztuQocpVtmzAeCwuAcVYiVd3pcq8srlJfDoWgkfVtLZg6oyCxrmSN7VQyv2O
4WHnItYdZZSlHSH4Af0IZizYc5C3yBh6f4Txv6qyFPKQ/9MOR3FTvZlxrQDxk3dHK8esRa32FrjVX/icCl
3k2M3p6x4=
```

DMARC Identifier Alignment

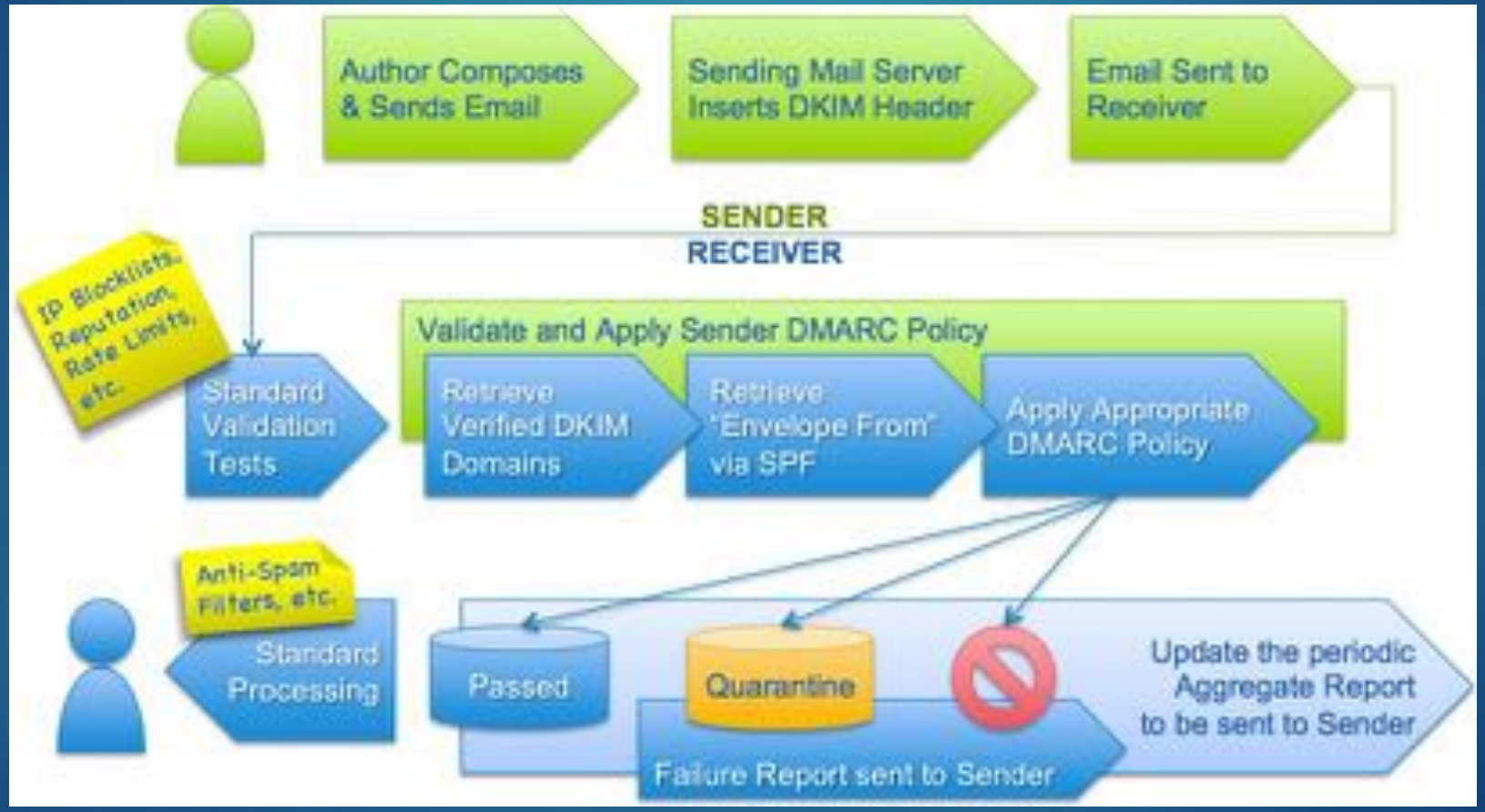
- RFC5322:From field
  - Email address of message author.
  - Usually present along with "Subject:“, "Date:" and the "To:" fields.
  - Is generally visible to recipient.

- Alignment with RFC5322:From field
  - DKIM - “d=“ must match domain in RFC5322:From field.
  - SPF - domain of RFC5322:From field must authorize sender in RFC5321.MailFrom field.
  - Either must be true to pass DMARC.

Authentication-Results: header

```
Authentication-Results: mx.google.com;
       dkim=pass header.i=@tvc.texas.gov header.s=selector1 header.b=fAkkbsj6;
       spf=pass (google.com: domain of peter.donton@tvc.texas.gov designates [redacted] as
permitted sender) smtp.mailfrom=peter.donton@tvc.texas.gov;
       dmarc=pass (p=NONE sp=NONE dis=NONE) header.from=tvc.texas.gov
```

Flow of Authentication



Deploying DMARC (for senders)

- Deploy DKIM and SPF
- Inventory all legitimate sources
  - Sub-domains
  - Third parties
- Publish DMARC record
  - Start out with p=none
- Analyze aggregate reports
- Adjust DMARC record accordingly

The _dmarc. TXT Record

Tag Name	Purpose	
v	Protocol version	v=DMARC1
pct	Percentage of messages subjected to filtering	default is 100
ruf	Reporting URI for forensic reports. Not so commonly generated due to volume and privacy.	ruf=mailto:abuse@example.com
rua	Reporting URI of aggregate reports	rua=mailto:report@example.com
p	Policy for organizational domain	none, quarantine, reject
sp	Policy for subdomains of the domain owner	sp=reject
adkim	Alignment mode for DKIM	Strict or Relaxed adkim=s
aspf	Alignment mode for SPF	String or Relaxed aspf=r

Example of domain with no outbound email

- _dmarc.tvc.state.tx.us.
  - v=DMARC1; p=reject; rua=mailto:dmarc.rua@tvc.state.tx.us; ruf=mailto:dmarc.ruf@tvc.state.tx.us
- v=spf1 -all
- selector1._domainkey.tvc.state.tx.us
  - v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDFs6yjlCZdRZeVzYfSnXz294hyxIPwhcHJQGmhU5p7LU1bKg39vhTIPxhoTCFt4cgq07n6QgcrMJlTAgEPlP+yUO57uwvvCFDm3yEBC2JyB3PN1SmRCFm//iyFxx2v7bxtc2JzH5Bci0VfVVISXDh4Qey8yBfUo+PnSulAxQ12TwIDAQAB; n=1024,1453121368,1

DMARC Reports

- Two types
  - Failure report
  - Aggregate report
- Receivers must implement mailto:
  - `rua=mailto:dmarc.rua@tvc.state.tx.us!50m`
  - `rua=mailto:dmarc.rua@tvc.state.tx.us,report@example.com`
- Destination domain must match owner domain
  - If not, TXT record with `v=DMARC1` at destination domain
  - `tvc.state.tx.us._report._dmarc.example.com`

Anatomy of Aggregate Report

- XML format in a ZIP file email attachment
- One RFC5322.From domain per report
- One or more record for each RFC5322.MailFrom IP address
- Supporting receivers send report at frequency in `ri=` tag in minutes
  - Default is daily
  - Ultimately, it is up to the receiver

Anatomy of Aggregate Report- report information

Anatomy of Aggregate Report- policy in effect

```
<?xml version="1.0" encoding="UTF-8" ?>
<feedback>
  <report_metadata>
  <policy_published>
    <domain>tvc.state.tx.us</domain>
    <adkim>r</adkim>
    <aspf>r</aspf>
    <p>reject</p>
    <sp>reject</sp>
    <pct>100</pct>
  </policy_published>
  <record>
</feedback>
```

Anatomy of Aggregate Report- sender IP and message count

Anatomy of Aggregate Report- record identifiers

```
<?xml version="1.0" encoding="UTF-8" ?>
<feedback>
  <report_metadata>
  <policy_published>
  <record>
    <row>
    <identifiers>
      <header_from>tvc.state.tx.us</header_from>
    </identifiers>
    <auth_results>
  </record>
</feedback>
```

Anatomy of Aggregate Report authentication results

Anatomy of Aggregate Report- alignment results

```
<?xml version="1.0" encoding="UTF-8" ?>
<feedback>
  <report_metadata>
  <policy_published>
  <record>
    <row>
      <source_ip>103.26.41.72</source_ip>
      <count>1</count>
      <policy_evaluated>
        <disposition>reject</disposition>
        <dkim>fail</dkim>
        <spf>fail</spf>
      </policy_evaluated>
    </row>
    <identifiers>
    <auth_results>
  </record>
</feedback>
```

Anatomy of Aggregate Report- a more interesting record

```
<record>
  <row>
    <source_ip>[redacted]</source_ip>
    <count>1</count>
    <policy_evaluated>
      <disposition>none</disposition>
      <dkim>fail</dkim>
      <spf>fail</spf>
    </policy_evaluated>
  </row>
  <identifiers>
    <header_from>tvc.texas.gov</header_from>
  </identifiers>
  <auth_results>
    <dkim>
      <domain>auth.ccsend.com</domain>
      <result>pass</result>
      <selector>1000073432</selector>
    </dkim>
    <spf>
      <domain>in.constantcontact.com</domain>
      <result>pass</result>
    </spf>
  </auth_results>
</record>
```

Anatomy of Aggregate Report- another interesting record

```
<record>
  <row>
    <source_ip>[redacted]</source_ip>
    <count>1</count>
    <policy_evaluated>
      <disposition>none</disposition>
      <dkim>fail</dkim>
      <spf>fail</spf>
    </policy_evaluated>
  </row>
  <identifiers>
    <header_from>tvc.texas.gov</header_from>
  </identifiers>
  <auth_results>
    <dkim>
      <domain>[redacted]</domain>
      <result>pass</result>
      <selector>[redacted]</selector>
    </dkim>
    <dkim>
      <domain>[redacted]onmicrosoft.com</domain>
      <result>pass</result>
      <selector>[redacted]</selector>
    </dkim>
    <spf>
      <domain>[redacted]</domain>
      <result>pass</result>
    </spf>
  </auth_results>
</record>
```

References and Resources

- RFC 7489 https://tools.ietf.org/html/rfc7489
- https://dmarc.org/resources/
- Messaging Malware Mobile Anti-Abuse Working Group
  - YouTube playlist of 6 DMARC training videos
- Tools
  - dmarcian.com/dmarc-tools/
  - mxtoolbox.com/dmarc.aspx
  - www.fraudmarc.com/dmarc-check/

Questions (hopefully answers)